Monday, March 5, 2018   **Latest:** Droopescan – Plugin Based CMS Security Scanner

HaXF4RALL
Hackers Repository

Grab your copy here

Download Hackers Handbook 2017

Follow Us

HAXF4RALL
9K likes

Like Page

Be the first of your friends to like this

News

Fileless WannaMine Cryptojacking Malware Using NSA Exploit

📅 February 5, 2018   👤 haxf4rall2017   💬 0 Comments   🏷 Fileless WannaMine Cryptojacking Malware Using NSA Exploit, wannamine tool, wannamine tutorial

Forget WannaCry and welcome WannaMine, a fileless cryptojacking malware using leaked NSA exploit called EternalBlue.

We cannot ignore the fact that cryptocurrencies are much in demand and monetary worth of digital currencies like Bitcoin, Ethereum, Litecoin, and Monero have soared tremendously, thereby, increasing the purchasing power and liquidity of cryptocurrency wallets.

with an extremely productive process known as mining. Through cryptocurrency mining, they can drain energies from even the most powerful computer systems.

Whats more disturbing is that now cybercriminals have come up with cryptojacking malware that is solely created to suck the CPU power from computers. One such cryptojacking malware is WannaMine. It uses leaked hacking tools of the NSA (National Security Agency) to gain access to computers and drain off processor power to carry out mining.

Here, we must recall the NSA's Windows exploit known as EternalBlue that was leaked in April 2017 by hacking group Shadow Brokers and was later used to launch the disastrous WannaCry ransomware that caused havoc worldwide and locked down NHS systems. WannaCry ransomware managed to infect around 230,000 computers in nearly 150 countries only to pave the way for another highly dangerous ransomware NotPetya. The same exploit is being used again to carry out Bitcoin and Monero mining using cryptojacking malware WanaMine.

WannaMine was identified by cybersecurity firm Panda in October 2017 while the malware was mining Monero after hijacking CPU cycles on the targeted computer. Another cybersecurity firm CrowdStrike stated that they have observed an increment in the distribution rate of WannaMine malware as infections caused by this malicious software have doubled in last few months. In fact, it crippled the operations of various companies for days and weeks and used the resources of their CPUs for Monero mining.

WannaMine is a fileless malware that utilizes advanced tactics and techniques to "maintain persistence within a network and move laterally from system to system. WannaMine uses credentials acquired with the credential harvester Mimikatz to attempt to propagate and move laterally with legitimate credentials." wrote CrowdStrike security researchers.

Hackers are using a wide range of techniques to infect computers from email phishing attacks to remote access hack. Using Mimikatz means that the machines patched against the notorious EternalBlue exploit previously won't be able to tolerate this malware too. "If unsuccessful, WannaMine attempts to exploit the remote system with the EternalBlue exploit," read the blog post by CrowdStrike researchers.

WannaMine uses built-in Windows components like Windows Management Instrumentation (WMI) and PowerShell to perform its malicious tasks. Since it is a fileless malware, hence, it becomes quite

Popular Posts

comparison to other malware like Adyllkuzz that require downloading of an application called CPUMiner to operate.

It is worth noting that WannaMine malware isn't as dangerous as NotPetya or WannaCry were because it does not lock the computers but it does drain off 100% of the IT environment capability of a client by excessively using the CPUs, which is concerning for firms running data centers or server farms.

While for individual users it would mean that their PCs or laptops' performance will deteriorate considerably. To protect your computers, it is important to enhance anti-virus security and install cybersecurity tools to ensure endpoint protection and mitigate WannaMine threat.

Advertisements

Share this:

10/8.1/7 (2017)

Free Burp Suite Hacking Course – Web Hacking Tool

Fappening 3.0 continues - Private Photos of Nicole Scherzinger, Dakota Johnson and Addison Timlin

CEH v9 – Certified Ethical Hacker v9 Course PDF + Tools DOWNLOAD

How to Bypass SMS Verification of any Website/Service

Freebitco.in script to Earn Free Bitcoin

Hackers Handbook 2017

Submit a Tool

Tricks & How To's

Like this:

⭐ **Like**

Be the first to like this.

Related

Shadow Brokers Leaks Another Windows Hacking Tool from NSA
September 8, 2017
In "News"

WikiLeaks Reveals 'AfterMidnight' & 'Assassin' CIA Windows Malware Frameworks
May 15, 2017
In "News"

5 Easy Ways To Block Cryptocurrency Mining In Your Web Browser
September 26, 2017
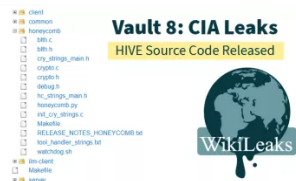In "Tricks & How To's"

← KeyBox – Open-source Web-based SSH Console

Hacking Germany – Computers, Cyber Attacks and The Future (Documentary Film) →

👍 You May Also Like

You Are Being Spied: Blame Your Beloved Apps
📅 September 20, 2015   💬
0

Vault 8 – Cia Leaks Project Hive Source Code
📅 November 10, 2017   💬
0

The Vigilante Hacker that hacked Hacking Team
📅 April 21, 2016   💬 1

Leave a Reply

Your email address will not be published. Required fields are marked *

Operating Systems can be detected using Ping Command

📅 February 24, 2018   👤 haxf4rall2017   💬 0

Ping is a computer network administration software utility, which used to find the Availability of a host on an Internet

Share this:

🐦 📘 7 G+

★ Like

Be the first to like this.

Build Your Own IPsec VPN Server: Auto Setup Scripts

📅 February 13, 2018   💬 0

How to Access Facebook Full Site

Desktop version on Android/iPhone Mobile browser

📅 January 13, 2018   💬 0

Freebitco.in script to Earn Free Bitcoin

📅 December 9, 2017   💬 4

35+ Unique Rainmeter Skins

📅 December 8, 2017   💬 1

Microsoft Toolkit – All in one Windows and Office Activator [Download]

📅 November 28, 2017   💬 0

SSH Tricks for Hackers

Name *

Email *

Website

Post Comment

☐ Notify me of follow-up comments by email.

☐ Notify me of new posts by email.

21, 2017

0

Hackers Handbook 2017

Grab your copy here

Social Media Hacking

SocialFish – Phishing Tool with Ngrok integrated

📅 February 7, 2018   👤
haxf4rall2017   💬 0

Socialfish uses ngrok to
secure the phishing URL to
your localhost.
Advertisements Related

Like this:

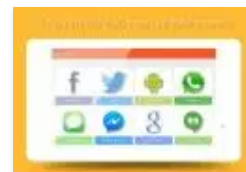Loading…

TeleShadow – Telegram Desktop Session Stealer

October 4, 2017   0

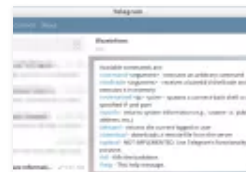### Using BeEF to Hack Facebook Credentials

June 20, 2017   0

How to make Fake Conversations on Popular Messenger Apps

May 16, 2017   0

Bt2 – Blaze Telegram Backdoor Toolkit

June 7, 2016   0

Courses & Ebooks

Free Burp Suite Hacking Course – Web Hacking Tool

📅 March 4, 2018   👤
haxf4rall2017   💬 0

This course will help you to master Burp Suite. If you are doing or wanting to do penetration testing, then

Like this:

Loading...

Free Penetration Testing Course

📅 February 12, 2018 💬 0

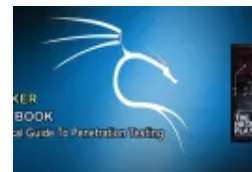### Ethical Hacking & Cyber Security Course : A Complete Package (FREE)

📅 January 9, 2018 💬 1

Kali Linux Hacking eBooks Download in PDF 2017

📅 November 28, 2017 💬 1

The Hacker Playbook: Practical Guide To Penetration Testing

📅 November 26, 2017 💬 0

Documentaries

Documentary

Hacking Germany – Computers, Cyber Attacks and The Future (Documentary Film)

📅 February 6, 2018   👤 haxf4rall2017   💬 0

Cyber attacks are common and show how vulnerable our digitally interconnected lives have become. Advertisements Related

Share this:

Like this:

Loading...

Cyber War (Documentary Film)

📅 January 31, 2018   💬 0

Defeating the Hackers (Documentary Film)

💬 0

Naked Citizens Documentary

📅 January 28, 2018   💬 0

Free the Network – Hackers Take Back the Web (Documentary Film)

📅 December 9, 2017   💬 0

About Us

Haxf4rall is a collective, a good starting point and provides a variety of quality material for cyber security professionals.

Useful Links

Contact Us

Disclaimer

Privacy Policy

Submit a Tool

Categories

Coding

Documentary
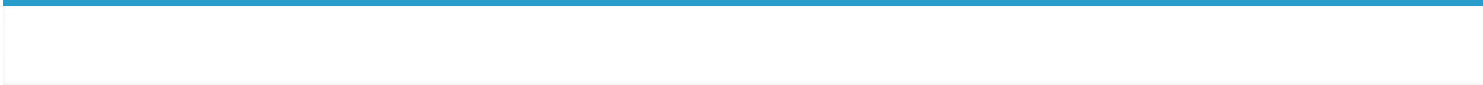
Courses & Ebooks

Hack Tools

Hacking Tutorials

Join Our Community!

Get the latest News and Hacking Tools delivered to your inbox.

News

Opensource

Operating Systems

TOR

Tricks & How To's

Don't Worry ! You will
not be spammed

Subscribe